REMARKS

Claims 1, 3-6, 8, 11, 13, 15-19, 22-24, 34 and 41-43 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel et al. (US Patent 7,159,149), and further in view of Willebeek-LeMair et al. (US Publication 2003/0204632). Claims 25, 27, 28 and 35 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel, and further in view of Willebeek-LeMair and Bunker et al. (US Publication 2003/0056116, hereinafter Bunker).

Amended independent claim 1 recites, among other things, a feature of:

> acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; and
>
> ...
>
> changing the setting information upon it being judged at the judging that the communication is executed by the worm,
>
> wherein the acquiring includes acquiring the information based on the setting information changed at the changing.

As will be explained below, at least these features of claim 1 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the features of claim 1 by asserting the following:

> For example, the threshold can specify a percentage increase over normal connection failures rates and/or destination address diversity. The WDS 100 thus declares a computer worm when it detects rates above these thresholds. <u>This technique allows for the threshold criteria to be dynamic</u>, adapting to the particular operating environment of each system.

(See Spiegel Column 5, lines 15-21, <u>underlining</u> added for emphasis)

> In another embodiment of the threshold criteria, the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. This allows the heuristic to be fine tuned, for example, to increase the indication of malicious behavior when a particular source 10,20 has a failed connection attempt to a suspect address.

(See Spiegel Column 5, lines 47-53, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(See Spiegel Column 6, lines 15-24, underlining added for emphasis)

Spiegel also describes the following:

> A worm is thus declared (i.e., that a particular source is infected with a worm) when the source's failed network connection attempts during a period of time meet or exceed at least one of the threshold criteria.

(See Spiegel Column 3, lines 63-67, underlining added for emphasis)

> Therefore, failed attempts to a small number of addresses may or may not indicate malicious behavior, but failed attempts to many addresses is a significant indicator of--and thus a good heuristic for--a computer worm.

(Column 4, lines 27-31, underlining added for emphasis)

However, Spiegel merely teaches that a worm is thus declared when the source's failed network connection attempts … meet or exceed at least one of the threshold criteria and “this technique allows for the threshold criteria to be dynamic”.

Spiegel fails to disclose or suggest the features of independent claim 1, such as the following:

> acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement;
>
> . . .
>
> changing the setting information upon it being judged at the judging that the communication is executed by the worm,
>
> wherein the acquiring includes acquiring the information based on the setting information changed at the changing.
>
> (underlining added for emphasis)

Hence, the noted features are also a distinction over Spiegel. The noted features also is a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a prima facie case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 1 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a prima facie case of obviousness vis-à-vis claim 1.

Claim 4 depends from claim 1, and so at least similarly distinguishes over Spiegel, and thus over its combination with Willebeek-LeMair.

Amended independent claim 3 recites, among other things, features of:

> changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm, wherein
>
> the judging includes further judging whether the communication is executed by the worm based on the information acquired and the judgment criteria changed at the changing.

As will be explained below, at least these features of amended claim 3 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the features of claim 3 by the following descriptions:

> In another embodiment, the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions. The threshold specifies a deviation from the normal operating conditions such that an observed actual condition outside this specified deviation is considered non-normal.

(See Spiegel Column 5, lines 8-15, underlining added for emphasis)

> For example, the threshold can specify a percentage increase over normal connection failures rates and/or destination address diversity. The WDS 100 thus declares a computer worm when it detects rates above these thresholds. This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system.

(See Spiegel Column 5, lines 15-21, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(See Spiegel Column 6, lines 15-24, underlining added for emphasis)

Spiegel also describes the following:

> A worm is thus declared (i.e., that a particular source is infected with a worm) when the source's failed network connection attempts during a period of time meet or exceed at least one of the threshold criteria.

(See Spiegel Column 3, lines 63-67, underlining added for emphasis)

> Therefore, failed attempts to a small number of addresses may or may not indicate malicious behavior, but failed attempts to many addresses is a significant indicator of--and thus a good heuristic for--a computer worm.

(See Spiegel Column 4, lines 27-31, underlining added for emphasis)

However, Spiegel merely teaches that a worm is thus declared when the source's failed network connection attempts ... meet or exceed at least one of the threshold criteria; and "this technique allows for the threshold criteria to be dynamic".

Spiegel fails to disclose or suggest the features of amended claim 3, such as:

> changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm, wherein
>
> the judging includes further judging whether the communication is executed by the worm based on the information acquired and the judgment criteria changed at the changing.
>
> (underlining added for emphasis)

Hence, the above noted features are a distinction over Spiegel. The noted features are also a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

In view of the distinction of claim 3 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a prima facie case of obviousness vis-à-vis claim 3.

Claim 41 depends from claim 3, and so at least similarly distinguishes over Spiegel, and thus over its combination with Willebeek-LeMair.

Amended independent claim 5 recites, among other things, features of:

> the second judging includes judging that a plurality of computers in the predetermined segment are infected by the worm when
>
> a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside, and
>
> a number of destination addresses of the communication packets that is are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging.

As will be explained below, at least these features of claim 5 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the features of claim 5 by the following descriptions:

> In another embodiment, the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions. The threshold specifies a deviation from the normal operating conditions such that an observed actual condition outside this specified deviation is considered non-normal.

(See Spiegel Column 5, lines 8-15, underlining added for emphasis)

> In another embodiment of the threshold criteria, the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. This allows the heuristic to be fine tuned, for example, to increase the indication of malicious behavior when a particular source 10,20 has a failed connection attempt to a suspect address.

(See Spiegel Column 5, lines 47-53, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring

> module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. <u>A module may be implemented in hardware, software, firmware, or any combination thereof</u>.

(See Spiegel Column 6, lines 15-24, <u>underlining</u> added for emphasis)

However, Spiegel fails to disclose or suggest the features of claim 5, such as:

> <u>the second judging includes judging that a plurality of computers in the predetermined segment are infected by the worm</u> when
>
> a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside, and
>
> a number of destination addresses of the communication packets that is are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging.
>
> (<u>underlining</u> added for emphasis)

Hence, the above noted features are a distinction over Spiegel. The noted features are also a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

In view of the distinction of claim 5 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a prima facie case of obviousness vis-à-vis claim 5.

Amended independent claim 8 recites, among other things, the feature of:

> the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that are recorded in advance.

As will be explained below, at least this feature of claim 8 is a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel and Willebeek-LeMair teach the features of claim 8 by the following descriptions:

> The heuristic for any of the embodiments can take a variety of forms, as the failed connection attempts associated with a particular source can be quantified in many ways. In one embodiment, the heuristic is implemented with a set of threshold criteria that embodies whether the failed connection attempts associated with a source are non-normal. A worm is thus declared (i.e., that a particular source is infected with a worm) when the source's failed network connection attempts during a period of time meet or exceed at least one of the threshold criteria. In various embodiments, the threshold criteria include any one or a combination of the following metrics: (1) the number of failed network connection attempts; (2) the diversity of destination network addresses associated with the failed network connection attempts; (3) the randomness of the failed addresses; and (4) a weighting for each failed network connection attempt according to an attribute thereof (e.g., source or destination address).

(Spiegel, Column 3, lines 58-67, underlining added for emphasis)

> In another embodiment, the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions. The threshold specifies a deviation from the normal operating conditions such that an observed actual condition outside this specified deviation is considered non-normal.

(Spiegel, Column 5, lines 8-15, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring

> module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(Spiegel, Column 6, lines 15-24, underlining added for emphasis)

> The system 10 further includes a signature database 20 that stores detection signatures 22 (comprising, for example, security rules, policies and algorithms) that are designed to mitigate or avert network damage from detected vulnerabilities. These signatures 22 may be obtained from any one of a number of well known sources, including, for example, machine (host) manufacturers, service suppliers, the Internet, and the like. Additionally, the signatures 22 may be created by an administrator 24 of the protected network 14. Still further, the signatures 22 may be supplied by a entity 26 in the business of signature creation, where that entity operates to collect threat information (for example, worm, virus, trojan, DoS, Access, Failure, Reconnaissance, other suspicious traffic, and the like) from around the world, analyze that information and design detection signatures 22 that can be used by others to mitigate or avert network damage from the collected threats.

(Willebeek-LeMair, Paragraph [0030], lines 1-17, underlining added for emphasis)

However, Spiegel and Willebeek-LeMair fail to disclose or suggest the following feature of claim 8,

> the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that are recorded in advance.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Spiegel or Willebeek-LeMair.

In view of the distinction of claim 8 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 8.

Claim 43 depends from claim 8, and so at least similarly distinguish over Spiegel, and thus over its combination with Willebeek-LeMair.

Amended independent claim 13 recites, amend other things, features of:

> acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; and
>
> ...
>
> changing the setting information upon it being judged at the judging that the communication is executed by the worm,
>
> wherein the acquiring includes acquiring the information based on the setting information changed at the changing

As will be explained below, at least these features of claim 13 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the features of claim 13 by the following descriptions:

> For example, the threshold can specify a percentage increase over normal connection failures rates and/or destination address diversity. The WDS 100 thus declares a computer worm when it detects rates above these thresholds. <u>This technique allows for the threshold criteria to be dynamic</u>, adapting to the particular operating environment of each system.

(See Spiegel Column 5, lines 15-21, <u>underlining</u> added for emphasis)

> <u>In another embodiment of the threshold criteria, the failed attempts are weighted</u> according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. This allows the heuristic to be fine tuned, for example, to increase the

> indication of malicious behavior when a particular source 10,20 has a failed connection attempt to a suspect address.

(See Spiegel Column 5, lines 47-53, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(See Spiegel Column 6, lines 15-24, underlining added for emphasis)

Spiegel also describes the following:

> A worm is thus declared (i.e., that a particular source is infected with a worm) when the source's failed network connection attempts during a period of time meet or exceed at least one of the threshold criteria.

(See Spiegel Column 3, lines 63-67, underlining added for emphasis)

> Therefore, failed attempts to a small number of addresses may or may not indicate malicious behavior, but failed attempts to many addresses is a significant indicator of--and thus a good heuristic for--a computer worm.

(See Spiegel Column 4, lines 27-31, underlining added for emphasis)

However, Spiegel merely teaches that a worm is thus declared when the source's failed network connection attempts … meet or exceed at least one of the threshold criteria; and "this technique allows for the threshold criteria to be dynamic". Spiegel fails to disclose or suggest the features of amended claim 13, such as:

> acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; and
>
> . . .
>
> changing the setting information upon it being judged at the judging that the communication is executed by the worm,
>
> wherein the acquiring includes acquiring the information based on the setting information changed at the changing

(underlining added for emphasis)

Hence, the above noted features are a distinction over Spiegel. The noted features are also a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

As discussed above, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 13 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 13.

Amended independent claim 15 recites, among other things, features of:

> an acquiring unit that acquires information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; and
>
> . . .
>
> a setting changing unit that changes the setting information upon it being judged by the judging unit that the communication is executed by the worm, wherein
>
> the acquiring unit acquires the information based on the setting information changed by the setting changing unit.

As will be explained below, at least these features of claim 15 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the features of claim 15 by the following descriptions:

> For example, the threshold can specify a percentage increase over normal connection failures rates and/or destination address diversity. The WDS 100 thus declares a computer worm when it detects rates above these thresholds. This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system.

(See Spiegel Column 5, lines 15-21, underlining added for emphasis)

> In another embodiment of the threshold criteria, the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. This allows the heuristic to be fine tuned, for example, to increase the indication of malicious behavior when a particular source 10,20 has a failed connection attempt to a suspect address.

(See Spiegel Column 5, lines 47-53, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(See Spiegel Column 6, lines 15-24)

Spiegel also describes the following:

> A worm is thus declared (i.e., that a particular source is infected with a worm) when the source's failed network connection attempts during a period of time meet or exceed at least one of the threshold criteria.

(See Spiegel Column 3, lines 63-67, underlining added for emphasis)

> Therefore, failed attempts to a small number of addresses may or may not indicate malicious behavior, but failed attempts to many addresses is a significant indicator of--and thus a good heuristic for--a computer worm.

(See Spiegel Column 4, lines 27-31, underlining added for emphasis)

However, Spiegel merely teaches that a worm is thus declared when the source's failed network connection attempts ... meet or exceed at least one of the threshold criteria; and "this technique allows for the threshold criteria to be dynamic". Spiegel fails to disclose or suggest the features of amended claim 15, such as:

> an acquiring unit that acquires information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; and
>
> ...
>
> a setting changing unit that changes the setting information upon it being judged by the judging unit that the communication is executed by the worm, wherein
>
> the acquiring unit acquires the information based on the setting information changed by the setting changing unit.
>
> (underlining added for emphasis)

Hence, the above noted features are a distinction over Spiegel. The noted features are also a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

In view of the distinction of claim 15 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 15.

Claim 17 depends from claim 15, and so at least similarly distinguishes over Spiegel, and thus over its combination with Willebeek-LeMair.

Amended independent claim 16 recites, amend other things, features of:

> a setting changing unit that changes the judgment criteria upon it being judged by the judging unit that the communication is executed by the worm, wherein
>
> the judging unit further judges whether the communication is executed by the worm based on the information acquired by the acquiring unit and the judgment criteria changed at the changing.

As will be explained below, at least these features of amended claim 16 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the feature(s) of claim 16 by the following descriptions:

> In another embodiment, the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions. The threshold specifies a deviation from the normal operating conditions such that an observed actual condition outside this specified deviation is considered non-normal.

(See Spiegel Column 5, lines 8-15, underlining added for emphasis)

> For example, the threshold can specify a percentage increase over normal connection failures rates and/or destination address diversity. The WDS 100 thus declares a computer worm when it detects rates above these thresholds. This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system.

(See Spiegel Column 5, lines 15-21, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(See Spiegel Column 6, lines 15-24, underlining added for emphasis)

Spiegel also describes the following:

> Therefore, <u>failed attempts to a small number of addresses may or may not indicate malicious behavior</u>, but failed attempts to many addresses is a significant indicator of--and thus a good heuristic for--a computer worm.

(See Spiegel Column 4, lines 27-31, <u>underlining</u> added for emphasis)

However, Spiegel merely teaches that a worm is thus declared when the source's failed network connection attempts ... meet or exceed at least one of the threshold criteria; and "this technique allows for the threshold criteria to be dynamic". Spiegel fails to disclose or suggest the features of amended claim 16, such as:

> <u>a setting changing unit that changes the judgment criteria upon it being judged</u> by the judging unit <u>that the communication is executed by the worm</u>, wherein
>
> the judging unit further judges whether the communication is executed by the worm based on the information acquired by the acquiring unit and the judgment criteria changed at the changing.

(<u>underlining</u> added for emphasis)

Hence, the above noted features are a distinction over Spiegel. The noted features are also a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

In view of the distinction of claim 16 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 16.

Amended independent claim 18 recites, among other things, the features of:

> the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm when
>
> a communication from a the computer in the predetermined network segment is judged to be infected by the worm at the first time,
>
> there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first time.

As will be explained below, at least these features of claim 18 are a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Spiegel teaches the features of claim 18 by the following descriptions:

> In another embodiment, the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions. The threshold specifies a deviation from the normal operating conditions such that an observed actual condition outside this specified deviation is considered non-normal.

(See Spiegel Column 5, lines 8-15, underlining added for emphasis)

> In another embodiment of the threshold criteria, the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. This allows the heuristic to be fine tuned, for example, to increase the indication of malicious behavior when a particular source 10,20 has a failed connection attempt to a suspect address.

(See Spiegel Column 5, lines 47-53, underlining added for emphasis)

> FIG. 3 shows an embodiment of the WDS 100, which comprises a group of operatively coupled modules including a network monitoring

> module 110, a logging module 120, a logged data module 130, a criteria data module 140, an analysis module 150, and a response module 160. As used herein, the term "module" refers to computer program logic and/or any hardware or circuitry utilized to provide the functionality attributed to the module. A module may be implemented in hardware, software, firmware, or any combination thereof.

(See Spiegel Column 6, lines 15-24, underlining added for emphasis)

However, Spiegel fails to disclose or suggest the features of claim 18, such as:

> the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm when
>
> a communication from a the computer in the predetermined network segment is judged to be infected by the worm at the first time,
>
> there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first time.

(underlining added for emphasis)

Hence, the above noted features are a distinction over Spiegel. The noted features are also a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

In view of the distinction of claim 18 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 18.

Amended independent claim 22 recites, among other things, a feature of:

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

As will be explained below, at least this feature of claim 22 is a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Willebeek-LeMair teaches the following features of claim 22 by the following descriptions:

> The inspection operation performed by the inspection agent 28 involves first extracting 38 from the traffic 30 certain packet features of interest for inspection. More specifically, the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like) and/or features 38(2) from the payload portion 36 (such as, for example, character strings, regular expressions, and the like).

(Willebeek-LeMair, Paragraph [0031], lines 5-14, underlining added for emphasis)

However, Willebeek-LeMair fails to disclose or suggest this feature of claim 22,

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Willebeek-LeMair. The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

In view of the distinction of claim 22 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 22.

Amended independent claim 23 recites, among other things, a feature(s) of:

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

As will be explained below, at least this features of claim 23 is a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Willebeek-LeMair teaches the following feature of claim 23 by the following description:

> The inspection operation performed by the inspection agent 28 involves first extracting 38 from the traffic 30 certain packet features of interest for inspection. More specifically, the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like) and/or features 38(2) from the payload portion 36 (such as, for example, character strings, regular expressions, and the like).

(Willebeek-LeMair, Paragraph [0031], lines 5-14, underlining added for emphasis)

However, Willebeek-LeMair fails to disclose or suggest this feature of claim 23,

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Willebeek-LeMair. The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

In view of the distinction of claim 23 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 23.

Amended independent claim 24 recites, among other things, a feature of:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the judging unit, and extracts, as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the judging unit.

As will be explained below, at least this feature of claim 24 is a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Willebeek-LeMair teaches the feature of claim 24 by the following description:

> The inspection operation performed by the inspection agent 28 involves first extracting 38 from the traffic 30 certain packet features of interest for inspection. More specifically, the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like) and/or features 38(2) from the payload portion 36 (such as, for example, character strings, regular expressions, and the like).

(Willebeek-LeMair, Paragraph [0031], lines 5-14, underlining added for emphasis)

However, Willebeek-LeMair fails to disclose or suggest the features of claim 24, such as:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the judging unit, and extracts, as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the judging unit.

(underlining added for emphasis)

Hence, the noted feature is a distinction over Willebeek-LeMair. The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a prima facie case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 24 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a prima facie case of obviousness vis-à-vis claim 24.

Amended independent claim 34 recites, among other things, a feature of:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm judging unit, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm.

As will be explained below, at least this feature of claim 34 is a distinction over Spiegel and Willebeek-LeMair.

The Examiner contends that Willebeek-LeMair teaches the feature of claim 34 by the following descriptions:

> The inspection operation performed by the inspection agent 28 involves first extracting 38 from the traffic 30 certain packet features of interest for inspection. More specifically, the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like) and/or features 38(2) from the payload portion 36 (such as, for example, character strings, regular expressions, and the like).

(Willebeek-LeMair, Paragraph [0031], lines 5-14, underlining added for emphasis)

However, Willebeek-LeMair fails to disclose or suggest the feature of claim 24, such as:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm judging unit, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Willebeek-LeMair. The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

In view of the distinction of claim 34 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 34.

Amended independent claim 25 recites, among other things, a feature of:

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

As will be explained below, at least this feature of claim 25 is a distinction over Spiegel, Willebeek-LeMair, and Bunker.

The Examiner contends that Bunker teaches the feature of claim 25 by the following description:

> The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; total number of vulnerabilities discovered; number of vulnerabilities discovered, by risk level; number of vulnerabilities that have not been addressed since previous assessment; number of vulnerabilities fixed since the previous assessment; and historical trending of vulnerability count graphically and in table format across a defined scope, possibly including more than one division or more than one network. Thus, the source of rising vulnerabilities may be readily identified.

(See Bunker Paragraph [0189], lines 1-11, underlining added for emphasis)

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities.

(See Bunker Paragraph [0215], lines 1-5, underlining added for emphasis)

> The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; summary graphical information on severity, cause, likely impact, and sill level needed to exploit vulnerabilities

(See Bunker Paragraph [0220], lines 8-12, underlining added for emphasis)

However, Bunker fails to disclose or suggest the following feature of claim 25,

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Bunker. The above noted feature also is a distinction over Spiegel or Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel or Willebeek-LeMair as disclosing the noted feature.

In view of the distinction of claim 25 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a prima facie case of obviousness vis-à-vis claim 25.

Amended independent claim 27 recites, among other things, a feature of:

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

As will be explained below, at least this feature of claim 27 is a distinction over Spiegel, Willebeek-LeMair and Bunker.

The Examiner contends that Bunker teaches the feature of claim 27 by the following descriptions:

> The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; total number of vulnerabilities discovered; number of vulnerabilities discovered, by risk level; number of vulnerabilities that have not been addressed since previous assessment; number of vulnerabilities fixed since the previous assessment; and historical trending of vulnerability count graphically and in table format across a defined scope, possibly including more than one division or more than one network. Thus, the source of rising vulnerabilities may be readily identified.

(See Bunker Paragraph [0189], lines 1-11, underlining added for emphasis)

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities.

(See Bunker Paragraph [0215], lines 1-5, underlining added for emphasis)

> The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities;

> summary graphical information on severity, cause, likely impact, and sill level needed to exploit vulnerabilities

(See Bunker Paragraph [0220], lines 8-12, underlining added for emphasis)

However, Bunker fails to disclose or suggest the following feature of claim 27,

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Bunker. The above noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel or Willebeek-LeMair as disclosing the noted feature.

In view of the distinction of claim 27 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 27.

Amended independent claim 28 recites, among other things, a feature of:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the judging unit, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

As will be explained below, at least this feature of claim 28 is a distinction over Spiegel, Willebeek-LeMaira and Bunker.

The Examiner contends that Bunker teaches the feature of claim 28 by the following descriptions:

> The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; total number of vulnerabilities discovered; number of vulnerabilities discovered, by risk level; number of vulnerabilities that have not been addressed since previous assessment; number of vulnerabilities fixed since the previous assessment; and historical trending of vulnerability count graphically and in table format across a defined scope, possibly including more than one division or more than one network. Thus, the source of rising vulnerabilities may be readily identified.

(See Bunker Paragraph [0189], lines 1-11, underlining added for emphasis)

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities.

(See Bunker Paragraph [0215], lines 1-5, underlining added for emphasis)

> The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; summary graphical information on severity, cause, likely impact, and sill level needed to exploit vulnerabilities.

(See Bunker Paragraph [0220], lines 8-12, underlining added for emphasis)

However, Bunker fails to disclose or suggest the following feature of claim 27:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is

> executed by the judging unit, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Bunker. The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel or Willebeek-LeMair as disclosing the noted feature.

In view of the distinction of claim 28 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 28.

Amended independent claim 35 recites, among other things, a feature of:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

As will be explained below, at least this feature of claim 35 is a distinction over Spiegel, Willebeek-LeMair and Bunker.

The Examiner contends that Bunker teaches the feature of claim 35 by the following descriptions:

> The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; total number of vulnerabilities discovered; number of vulnerabilities

> discovered, by risk level; number of vulnerabilities that have not been addressed since previous assessment; number of vulnerabilities fixed since the previous assessment; and historical trending of vulnerability count graphically and in table format across a defined scope, possibly including more than one division or more than one network. Thus, the source of rising vulnerabilities may be readily identified.

(See Bunker Paragraph [0189], lines 1-11, underlining added for emphasis)

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities.

(See Bunker Paragraph [0215], lines 1-5, underlining added for emphasis)

> The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; summary graphical information on severity, cause, likely impact, and sill level needed to exploit vulnerabilities.

(See Bunker Paragraph [0220], lines 8-12, underlining added for emphasis)

However, Bunker fails to disclose or suggest the following feature of claim 35:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(underlining added for emphasis)

Hence, the above noted feature is a distinction over Bunker. The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel or Willebeek-LeMair as disclosing the noted feature.

In view of the distinction of claim 35 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 35.

In view of the foregoing discussion, the rejections of claims 1, 3-5, 8, 13, 15-18, 22-25, 27, 28, 34, 35, 41 and 43 is traversed, and withdrawal of the §103(a) rejection is respectfully requested.

For all of the foregoing reasons, Applicants submit that this Application is in condition for allowance, which is respectfully requested. The Examiner is invited to contact the undersigned attorney if an interview would expedite prosecution.

If a Petition under 37 C.F.R. §1.136(a) for an extension of time for response is required to make the attached response timely, it is hereby petitioned under 37 C.F.R. §1.136(a) for an extension of time for response in the above-identified application for the period required to make the attached response timely. The Commissioner is hereby authorized to charge any additional fees which may be required to this Application under 37 C.F.R. §§1.16-1.17, or credit any overpayment, to Deposit Account No. 07-2069.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By Joseph P. Fox
Joseph P. Fox
Registration No. 41,760

March 30, 2009
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
(312) 360-0080
Customer No. 24978